UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/574,345 | 05/19/2000 | Derek C. Au | 28189.00010 | 8281 |

25224 7590 12/23/2003

MORRISON & FOERSTER, LLP
555 WEST FIFTH STREET
SUITE 3500
LOS ANGELES, CA 90013-1024

| EXAMINER | |
|---|---|
| SHIN, KYUNG H | |
| **ART UNIT** | **PAPER NUMBER** |
| 2132 | 10 |

DATE MAILED: 12/23/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/574,345 | AU ET AL. | |
| | Examiner | Art Unit | |
| | Kyung H Shin | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *19 May 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☒ Claim(s) *7,20* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 May 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. §§ 119 and 120**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5,8* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

## DETAILED ACTION

### *Claim Objections*

1. The abstract of the disclosure is objected to because the abstract contains less than 50 words. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc. See MPEP § 608.01(b).

2. **Claim 7** is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim 6 and 4. See MPEP § 608.01(n). Accordingly, the claim 7 not been further treated on the merits.

3. **Claim 20** is objected to as being in improper form because it depends its own claim 20. A series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim. A claim, which depends from a dependent claim,

should not be separated by any claim that does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claims 1-~~22~~** 1,4-19 and 21-22 are rejected under 35 U.S.C. 102(b) as being anticipated by Jones (U.S. Patent No. 5,412,730).

**Regarding Claim 1, 10, 19** and **21**, Jones discloses a pseudo-random key generator for use within a cryptographic communication system, said pseudo-random key generator comprising: (Fig. 1 and Fig. 4)

a) a pseudo-random number generator; and (col. 3, line 27)

b) a computer readable storage medium connected to said pseudo-random number generator. (col. 4, line 40, and col. 9, line 53)

**Regarding Claim 4** (Amended)**, 5, and 6,** Jones discloses the cryptographic communication system according to claim 1, wherein said computer readable storage

(Fig. 4, col. 8, line 7) medium includes a PRN re-map table (col. 10, lines 6-9), a key block formation table. (col. 10, line 46) and timing circuit (Fig. 4, numeral 21).

**Regarding Claim 8** (Amended), Jones discloses the cryptographic communication system according to claim 6, wherein said computer readable storage medium includes an executable program, (col. 11, lines 11-18) causing said systems re-map generator to re-map the data of PRN re-map table. (col. 2, lines 8-24)

**Regarding Claim 9**, Jones discloses the cryptographic communication system according to claim 8, wherein said systems re-map generator selectively rearranges data stored in said computer readable storage medium. (col. 10, lines 21-29)

**Regarding Claim 10 (Amended)**, Jones discloses a cryptographic communication system having a pseudo-random key generator (Fig. 4, numeral 23) for generating cryptographic keys, said pseudo-random key generator comprising:

a) a pseudo-random number generator, (Fig. 4, numeral 38)

b) a timing circuit operatively coupled to said pseudo-random number generator; (Fig. 4, numeral 21)

c) a first computer readable storage area operatively coupled to said pseudo-random number generator, said first computer readable storage area containing a plurality of data values, each data value associated with a unique storage address within said first computer readable storage area: (col. 4, lines 35-43)

d) a second computer readable storage area operatively coupled to said first computer readable storage area, said second computer readable storage area containing a plurality of key data values, each key data value associated with a unique storage address within said second computer readable storage area, (col. 9, lines 55-60)

e) wherein the pseudo-random number generator periodically generates a pseudo-random number in accordance with the timing circuit, wherein each generated pseudo-random number is used to look up a unique address in the first computer readable storage area for retrieving the data value associated with the looked up unique address, and wherein the retrieved data value is used to look up a unique address in the second computer readable storage area for retrieving a key value data, said key value data being used to form a cryptographic key. (col. 9, lines 51-62)

**Regarding Claim 11 and 13 (Twice Amended)**, Jones discloses the cryptographic communication system according to claim 10, further comprising a programmed processor operatively coupled to said first/second computer readable storage area for generating the data values in accordance with a predetermined algorithm. (col. 10, lines 61-65)

**Regarding Claim 12, 14 and 16 (Twice Amended)**, Jones discloses the cryptographic communication system according to claim 11, wherein said programmed processor selectively rearranges the data values in said first/second computer readable storage area. (col. 10, line 66 - col. 11, line 8 )

**Regarding Claim 15**, Jones discloses a method of generating cryptographic keys using a pseudo-random number generator, a first/second computer readable storage area, said method comprising the steps of:

a) inputting into said pseudo-random number generator an initial data value; (col. 3, lines 26-33)

b) generating a pseudo-random numerical value; (col. 3, lines 33-36)

c) generating a first data string by using said generated pseudo-random numerical value to look up a unique memory address in the first computer readable storage area (col. 10, line 7) and retrieving a data value associated with the unique memory address in the first compute readable storage area, said data value being one of a plurality of data values stored in the first computer readable storage area; and (col. 9, lines 29-44)

d) generating a second data string by using said first data string to look up a unique memory address in the second computer readable storage area (col. 10, line 7) and retrieving a key data value associated with the unique memory address in the second compute readable storage area, said key data value being one of a plurality of key data values stored in the second computer readable storage area, (col. 9, lines 44-50)

e) wherein the retrieved key data value is used to form a cryptographic key. (col. 2, lines 8-24)

**Regarding Claim 17** (Amended), Jones discloses the method according to claim 15, further comprising the step of initializing said pseudo-random number generator. (col. 3, line 33)

**Regarding Claim 18**, Jones discloses the method according to claim 15, further comprising the step of initializing said computer readable storage area. (col. 12, line 6)

**Regarding Claim 22** (Amended), Jones discloses the cryptographic communications system according to claim 21, wherein each of said pseudo-random key generator includes a unique systems seed value. (col. 3, line 32)

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claim 2, 3** and **20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones (U.S. Patent No. 5,412,730) in view of Dent et al, (U.S. Patent No. 5,060,266).

Jones does not explicitly disclose "time clock" to supply input of pseudo-random number generator although "block counter" was indicated. Dent in analogous art

discloses "a time clock or block counter" (Fig. 5, numeral 201) to generate a count in response to an increment applied at the input, and generates a plurality of pseudo-random key stream bits.

**Regarding Claim 2** and **20**, Dent discloses the cryptographic communication system, further comprising timing circuit (Fig. 5, numeral 201) connected to said pseudo-random number generator. (col. 11, line 21)

**Regarding Claim 3**, Dent discloses the cryptographic communication system according to claim 1, wherein said timing circuit further comprises:

a) a time clock connected to said pseudo-random number generator;
a block /delta counter connected to said clock; and a time/key initialize device connected to said delta counter. (col. 10, line 63 - col. 11, line 22)

It would have been obvious to those of ordinary skill in the art at the time the invention was made to include therein "a time clock or block counter" (col. 11, line 60) generating input to the pseudo-random key generator of Jones as taught in Dent. One of ordinary skill in the art would have been motivated to use "a time clock or block counter" (Fig. 5, numeral 201) for the seed values of pseudo-random key generator in order to synchronize with transmitter counter in cryptographic communication.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is 703-305 -0711. The examiner can normally be reached on 6:30 am - 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-2394.

KHS

Kyung H Shin
Patent Examiner
Art Unit 2132

KHS
December 12, 2003

Gilberto Barron

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100